OFFICE OF THE CHIEF INFORMATION OFFICER

SERVICES DEVELOPMENT AND OPERATIONS DIVISION

SECURITY OPERATIONS BRANCH

COMPUTER SECURITY INCIDENT RESPONSE POLICY

VERSION 3.0

This page intentionally left blank.

Document History

Date	Version	Description	Authorization
Apr. 14, 2017	1.0	• Initial Release	Mike Williams
Dec. 28, 2017	1.1	• Confirmed policy references • Updated acronyms • Reconfirmed procedure accuracy	Mike Williams
June 4, 2018	1.2	• Updated document • Formatted document	Mike Williams
July 19, 2018	1.8	• Formatted document • Added title page and table of contents • Updated all pages	Mike Williams
September 28, 2018	1.9	• Updated document with reference to Federal Incident Notification Guidelines (FING) Draft 2 FY2019	Mike Williams
December 12, 2018	2.0	• Updated document with reference to OMB M-19-02 and Federal Incident Notification Guidelines (FING) Draft 2 FY2019	Mike Williams
June 11, 2019	3.0	• Bi-annual update • Updated document with reference to Federal Incident Reporting Requirements (FIRR) Draft	Mike Williams

Table of Contents

1.0 Purpose 1
2.0 Scope 1
3.0 References 1
4.0 Computer Security Incident Response Policy 2
5.0 Reporting Requirements 3
5.1 Incident Notification 4
5.2 Impact Classifications 5
5.3 Impact Description 5
4.4 Level of Impact 8
6.0 Incident Response Roles and Responsibilities 8
6.1 Computer Security Incident Response Team 8
6.2 SOB Chief and Team Leader 9
6.3 NRC Customer Support Center 10
6.4 Chief Information Security Officer 10
6.5 Chief Information Officer 11
6.6 NRC Users 11
6.7 Office of Administration 11
6.8 Office of Public Affairs 11
6.9 Office of General Counsel 11
6.10 Office of Congressional Affairs 11
6.11 Office of Inspector General 11
7.0 Frequency of Review 11
8.0 Cognizant Authority 11

Table 1: Functional Impact 5
Table 2: Information Impact 6
Table 3: Recoverability 6

1.0 PURPOSE

The Computer Security Incident Response Policy (CSIRP) meets the requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 4 to address the purpose, scope, roles, responsibilities, management commitment, coordination and federal compliance of the Nuclear Regulatory Commission (NRC) Computer Security Incident Response Capability (CSIRC).

CSIRC has become an important component of Information Technology (IT) programs. Security-related threats have not only become more numerous and diverse but also more damaging and disruptive. New types of computer security-related incidents emerge frequently. Based on the results of risk assessments, preventative activities can lower the number of computer security incidents but not all. Therefore, a CSIRC is necessary for proactively identifying potential threats (such as a new virus), rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited and restoring computing services. CSIRC is a team effort requiring strong coordination among all parties involved in the process.

This document provides NRC's policy for responding to computer security events affecting NRC's infrastructure, networks and users. This policy is stored in ADAMS as ML18219A422.

2.0 SCOPE

This CSIRP does not apply to classified and Safeguard Information (SGI) systems.

This is an addendum to the "Cybersecurity Incident Management" policy requirements in the NRC Management Directive 12.5: "NRC Cybersecurity Program" (Directive Handbook 12.5). The requirements affect all NRC employees, contractors, vendors and agents (users) having access to any system that resides at any NRC facility, contractor facility and/or the NRC network or storing any public or non-public NRC data.

Because effective computer security incident response (IR) is resource intensive, establishing a successful IR capability requires significant planning and resources. Continually monitoring threats through Intrusion Detection Systems (IDS) and other mechanisms is essential. Establishing documented procedures for assessing the current and potential business impact of computer security events is critical, as is implementing effective methods of collecting, analyzing and reporting data regarding those events. Employee networking and establishing suitable means of communication with other internal groups such as the Office of Chief Human Capital Officer (OCHCO), Office of the Inspector General (OIG), Office of the General Counsel (OGC) and with external groups such as other IR teams and law enforcement are vital.[1]

3.0 REFERENCES

The following policy and procedure documents are used throughout the CSIRP.

1. Committee on National Security Systems (CNSS) Policy No. 18 – *National Policy on Classified Information Spillage*, June 2006
2. Committee on National Security Systems (CNSS) Policy No. 1001 – *National Instruction on*

[1] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2., *Computer Security Incident Handling Guide*, August 2012
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Classified Information Spillage, February 2008

3. United States Nuclear Regulatory Commission (NRC) - Computer Security Incident Response Team (CSIRT) Standard Operating Procedures (SOP), June 2019

4. United States Government - Federal Information Security Modernization Act (FISMA) of 2014

5. National Institute of Standards and Technology (NIST) – NIST Special Publication (SP) 800-53 Rev. 4: *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013

6. National Institute of Standards and Technology (NIST) - NIST Special Publication (SP) 800-61 Rev. 2 - *Computer Security Incident Handling Guide*, August 2012

7. Executive Office of the President – Office of Management and Budget (OMB) Memorandum M-19-02*: Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, October 2018

8. Executive Office of the President - Office of Management and Budget (OMB) Memorandum M-17-12: *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 2017

9. United States Nuclear Regulatory Commission (NRC) - Management Directive 12.5 - *NRC Cybersecurity Program*, November 2017

10. Cybersecurity and Infrastructure Security Agency (CISA) – *US-CERT Federal Incident Notification Guidelines (FING)*, April 2017

11. Cybersecurity and Infrastructure Security Agency (CISA) - *Federal Incident Reporting Requirements (FIRR) Draft 1*

12. United States Code - 44 U.S.C. § 3552(b)(2)*, 2012 Edition, Supplement 3*, *Title 44 - PUBLIC PRINTING AND DOCUMENTS*, 2015

13. Nuclear Regulatory Commission (NRC) – Computer Security Incident Response Plan, June 2019

4.0 COMPUTER SECURITY INCIDENT RESPONSE POLICY

The Security Operations Branch (SOB) Chief, within the Office of the Chief Information Officer (OCIO) and Services Development Operations Division (SDOD), is responsible for ensuring development of a CSIRP that provides high level guidelines to support:

- NRC's CSIRC process:[2]
  - Preparation: selecting tools, preparing for computer security events and preventing incidents
  - Detection and Analysis: computer security incident categories, signs of an

[2] NIST SP 800-61 Rev. 2., *Computer Security Incident Handling Guide*, August 2012 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

incident, sources of precursors and indications, incident analysis, incident documentation, incident prioritization and incident notification

- Containment: containment strategy, evidence gathering and handling, identifying the attacker, etc.
- Eradication: deleting malicious code, disabling breached user accounts, etc.
- Recovery: restoring the system to normal operation and hardening the system to prevent similar computer security incidents
- Post Incident Activity: lessons learned using collected incident data, evidence retention, residual risk assessment and recommendations for improvement
- Incident Handling Checklist
- Recommendations

- Compliance with the Department of Homeland Security (DHS) US Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines (FING)[3]
- The CSIRP must be updated at least bi-annually or as needed (e.g. major change).

5.0 REPORTING REQUIREMENTS

The Federal Information Security Modernization Act (FISMA) of 2014 requires Federal agencies to establish CSIRC and report on required activities. OMB Memorandum M-19-02[4] describes the processes for Federal agencies to report to OMB and where applicable, the DHS.

The NRC must designate a primary and secondary point of contact (POC) with US-CERT, report incidents meeting the specific criteria and internally document corrective actions and their impact. OMB has also required the reporting of any release of personally identifiable information (PII), either in electronic or physical form, where that information may be accessed by those without a need-to-know. Each agency must determine how to best meet these requirements. PII spills in physical form must be reported to the Office of Administration (ADM) Division of Facilities and Security (DFS).

An "incident" is defined under FISMA as "an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."[5] NIST SP 800-61 Rev. 2 describes a computer security incident as a “violation or imminent threat” to “computer security policies” or “standard security practices.”[6]

OMB Memorandum M-19-02 defines a "major incident" as “any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the

[3] Cybersecurity and Infrastructure Security Agency, *United States Computer Emergency Readiness Team (US-CERT) Federal Incident Notification Guidelines*, April 2017
https://www.us-cert.gov/incident-notification-guidelines
[4] Executive Office of the President, Office of Management and Budget (OMB) Memorandum M-19-02: *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, October 2018
https://www.whitehouse.gov/wp-content/uploads/2018/10/M-19-02.pdf
[5] Federal Information Security Modernization Act of 2014, 44 USC § 3552(b)(2), December 2014
https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[6] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2., *Computer Security Incident Handling Guide*, August 2012
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

United States or to the public confidence, civil liberties, or public health and safety of the American people"; another definition of a "major incident" provided by the same memorandum is that it is "a breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstratable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people."[7]

A "breach" is defined as "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose."[8]

If Official Use Only (OUO), Sensitive Unclassified Non-Safeguard Information (SUNSI), and/or SGI data was not identified as such when submitted, then the release did not violate NRC's processes or procedures and would not be considered a spill that must be reported. However, the owner should be notified and remedial action should be taken to remove the information if required.

5.1 Incident Notification

Notifying US-CERT of a computer security incident is mandatory when the confidentiality, integrity or availability of a Federal Government information system is confirmed to be compromised by an unauthorized party. It is recommended that cyber events such as passive scans, phishing attempts, attempted access or thwarted exploits, should be reported to US-CERT if they have been under investigation for 72 hours. NRC should identify the threat vector and potential indicators of compromise before any mandatory notification or voluntary report.

> **Requirement:** US-CERT must be notified of all computer security incidents involving a Federal Government information system with a confirmed impact to confidentiality, integrity or availability within one hour of being positively identified by the agency's top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC) or Information Technology (IT) department.[9] Follow-on updates are required every 72 hours until the incident is resolved.

It is imperative for reporting agencies to adhere to the one-hour timeframe and provide all available information. Reporting must not be delayed in order to provide further details (i.e., root cause, vulnerabilities exploited or mitigation actions taken) as this may result in high risk to the system or enterprise. If the cause of the incident is later identified, the threat vector may be updated in a follow-up report.

Incidents should be reported to US-CERT based on reporting requirements in the CISA FIRR.

Reporting to Law Enforcement, OIG, OGC

When responding to a breach, the Chief Information Security Officer (CISO) shall coordinate with the

[7] OMB Memorandum M-19-02: *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, October 2018
https://www.whitehouse.gov/wp-content/uploads/2018/10/M-19-02.pdf
[8] OMB Memorandum M-17-12: *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 2017
https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf
[9] CISA, *US-CERT Federal Incident Notification Guidelines*, April 2017
https://www.us-cert.gov/incident-notification-guidelines
and CISA *Federal Incident Reporting Requirements (FIRR) Draft*

identified agency officials to ensure that law enforcement, OIG and OGC receive timely notifications. When appropriate, the OIG will notify law enforcement (e.g., FBI) when involvement is necessary. The CISO shall also consider and advise appropriate officials on whether the specific circumstances and/or type of PII are potentially compromised by a breach and require the involvement of other oversight entities.[10]

Reporting to Congress

NRC will notify the appropriate Congressional Committees - pursuant to FISMA - no later than seven days after the date in which there is a reasonable basis to conclude that a breach that constitutes a "major incident" has occurred. In addition, NRC shall also supplement the initial seven day notification to Congress with a report no later than 30 days after the agency discovers the breach. This notification shall be consistent with FISMA and OMB standards on reporting a breach to Congress. The NRC PII Breach Notification Policy shall identify the NRC officials responsible for notifying Congress.[11]

5.2 Impact Classifications

The tables below identify the impact of the incident, which may affect multiple types of data. The reporting organization must define the specific thresholds for loss of service availability (i.e., all, subset, loss of efficiency).

> **Note:** NRC refrains from reporting incidents involving non-cyber PII exposures or classified data spillage (e.g., unsecured hard copies) to US-CERT. NRC notifies the Freedom of Information Act (FOIA) Privacy Officer of all non-cyber incidents involving PII.

These tables are based on the CISA FIRR Draft.

5.3 Impact Description

Table 1: Functional Impact

Category Level	Category Description
No Impact	Event has no impact.
No Impact To Services	Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers.
Minimal Impact To Non-Critical Services	Some small level of impact to non-critical systems and services.
Minimal Impact To Critical Services	Minimal impact but to a critical system or service, such as email or active directory.
Significant Impact To Non-Critical Services	A non-critical service or system has a significant impact.

[10] OMB Memorandum M-17-12: *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 2017
https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf
[11] OMB Memorandum M-17-12: *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 2017
https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

Denial Of Non-Critical Services	A non-critical system is denied or destroyed.
Significant Impact To Critical Services	A critical system has a significant impact, such as local administrative account compromise.
Denial Of Critical Services/Loss Of Control	A critical system has been rendered unavailable.

Table 2: Information Impact

Category Level	Category Description
No Impact	No known data impact.
Suspected But Not Identified	A data loss or impact to availability is suspected, but no direct confirmation exists.
Privacy Data Breach	The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised.
Proprietary Information Breach	The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
Destruction Of Non-Critical Systems	Destructive techniques (such as master boot record (MBR) overwrite) have been used against a non-critical system.
Critical Systems Data Breach	Data pertaining to a critical system has been exfiltrated.
Core Credential Compromise	Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated.
Destruction Of Critical System	Destructive techniques, such as MBR overwrite, have been used against a critical system.

Table 3: Recoverability

Category Level	Category Description
Regular	Time to recovery is predictable with existing resources.
Supplemented	Time to recovery is predictable with additional resources.
Extended	Time to recovery is unpredictable; additional resources and outside help are needed.
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).

4.4 Level of Impact

Agencies should determine the level of impact of the incident by using the existing incident management process established in NIST SP 800-61 Rev. 2. NRC uses the National Cybersecurity and Communications Integration Center (NCCIC) Cyber Incident Scoring System (NCISS), which has the following categories:[12]

- Functional Impact
- Observed Activity
- Location of Observed Activity
- Actor Characterization
- Information Impact
- Recoverability
- Cross-Sector Dependency
- Potential Impact

6.0 INCIDENT RESPONSE ROLES AND RESPONSIBILITIES

This section summarizes the roles and responsibilities of NRC personnel responding to and reporting computer security incidents.

6.1 Computer Security Incident Response Team

SOB provides the CSIRC, which includes a centralized CSIRT that can assemble resources as needed from appropriate parts of NRC. The CSIRT Senior Watch Officer and Watch Officers are dedicated staff whose primary purpose is to address computer security incidents.

The SOB personnel staff the positions in CSIRT. The SOB team members' highest priority is the CSIRT responsibilities (compared to their other duties). Staff from the Office of Nuclear Security and Incident Response (NSIR) and ADM will be made available in an expeditious manner to support the CSIRT efforts. The CSIRT personnel receives specialized training annually, including simulated events, to facilitate effective responses during crisis situations. As appropriate, annual training will include automated mechanisms to provide a more robust and realistic training environment.

The CSIRT is responsible for summarizing all computer security incidents and all PII incidents (whether the compromise was electronic) in a report, transmitting this report to the CISO for approval and notifying US-CERT about malicious or suspicious activity that is confirmed by the NRC.

All confirmed incidents involving PII that are compromised by an unauthorized party must be reported to the NRC Senior Agency Official for Privacy (SAOP) and to US-CERT within one hour of being positively identified by NRC. All confirmed information spillages must be promptly reported.

Classified computer security incidents must follow the Committee on National Security Systems (CNSS) polices including, but not limited, to CNSS Policy No. 18 and CNSS Instruction No. 1001.

[12] CISA, *NCCIC Cyber Incident Scoring System*
https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System

The SOB Chief provides recommendations to the CISO on whether or not law enforcement or the OIG is needed to address computer security incidents. The SOB Chief and Team Leader are responsible for testing the NRC CSIRC bi-annually to determine capability effectiveness, document results and apply lessons learned for continuous CSIRC improvement. Whenever possible, the SOB Chief's testing of the CSIRC will include automated mechanisms to thoroughly evaluate the organization's IR process.

Specific CSIRT responsibilities include, but are not limited to:

- Immediate notification to the SOB Chief and the CISO of any US-CERT reportable computer security or PII incident.
- Immediate notification of PII or privacy incidents to the FOIA Privacy Officer.
- Making recommendations (as applicable) to the SOB Chief if law enforcement or the NRC OIG involvement is needed to address potential criminal or computer security incidents involving waste, fraud and abuse.
- Reporting computer security incident(s) directly to external groups such as US-CERT or law enforcement within the time frame required by federal guidance if NRC management is unavailable to give their approval. Law enforcement contact will be made through standard channels if necessary.
- Developing and maintaining procedures for computer security incident handling and reporting based on the CSIRT SOP.
- Developing and maintaining standards to ensure that an adequate audit trail exists to support the organization's computer security incident handling process.
- Developing and maintaining guidelines for communication with outside parties regarding incidents or CSIRT information.
- Confiscating or disconnecting equipment as required to prevent further computer security incidents or damage to NRC systems.
- Employing automated mechanisms to support/assist the computer security incident handling process, security incident tracking, collection of incident information, maintenance of a "chain of custody", analysis of computer security incident information and incident reporting.
- Establishing and maintaining relationships with internal organizations (e.g., OGC) and external groups (e.g., DHS).
- Responding, tracking and documenting computer security incidents on an ongoing basis (24 hours, seven days a week and 365 days a year).
- The CSIRT Team Leader is responsible for ensuring these responsibilities are fulfilled.

6.2 SOB Chief and Team Leader

Specific responsibilities include, but are not limited to:

- Providing oversight and guidance for the organization's CSIRC process and CSIRT activities.
- Providing staffing for the IR Hotline 24/7. The Senior Watch Officer is responsible for handling all incidents; the Senior Watch Officer will also delegate the responsibility of investigating, mitigating, resolving and reporting of the incidents to the primary incident handlers based on the monthly duty roster.

- Developing and maintaining a CSIRT based on Federal regulations, standards and guidelines.
- Raising any issues with the organization's CSIRC process with the CISO.
- Reviewing and approving all formal policies, procedures and best practices relating to computer security IR.
- Reviewing and approving all routine and periodic CSIRC reports before they are sent to the CISO or other Federal agencies.
- Evaluating all computer security incidents and making recommendations to the CISO if the involvement of law enforcement, OIG, OGC or a report to Congress is needed.
- Deciding if the involvement of law enforcement, OIG or OGC is necessary to mitigate the computer security incident if the CISO is not available to do so.
- Notifying the CIO if law enforcement, OIG, OGC or Congress should be contacted if the CISO is not available.
- Testing the CSIRC at least bi-annually to determine the capabilities' effectiveness.
- The SOB Chief will update the CSIRP at least bi-annually or as needed.
- The Computer Security IR Plan will identify procedures and capacities for cyber situational awareness visibility.

6.3 NRC Customer Support Center

The NRC Customer Support Center (CSC or Helpdesk) is responsible for reporting any actual or potential computer security incidents and all actual or potential PII incidents when they are recognized. A computer security or PII incident, verified or suspected, must be immediately reported to the NRC CSIRT. Prompt reporting of a suspected incident is essential in limiting damage resulting from the incident. The CSIRT can be contacted directly at (301) 415-6666 or CSIRT@nrc.gov.

Additional duties for the CSC are as follows:

- Analyzing and evaluating incoming calls for malicious or suspicious activity.
- Notifying the NRC CSIRT immediately if malicious or suspicious activity has been identified.

6.4 Chief Information Security Officer

Specific responsibilities include, but are not limited to:

- Ensuring that all IR issues raised by the SOB Chief are addressed.
- Reviewing periodic CSIRC reports and all reports sent to other Federal agencies.
- Reviewing and approving all IR reports if the incidents have been prioritized as "high".
- Deciding if the involvement of law enforcement, OGC and/or OIG is necessary to mitigate or address the computer security incident.
- Deciding whether or not to allow the operations of an information system to take place after a high-level computer security incident has occurred.
- Approving the CSIRC procedures that the agency uses.
- Notifying the CIO, if appropriate, of the nature of the incident.
- Notifying the CIO if law enforcement and/or OIG is contacted.

- Notifying the CIO if notification to the general public and the Office of Public Affairs (OPA) is required.
- Notifying the CIO and the Office of Congressional Affairs (OCA) if notification to Congress is required.
- Notifying the Executive Director for Operations (EDO), OPA and Commission as appropriate, and if the CIO is unavailable to do so.

6.5 Chief Information Officer

Specific responsibilities include, but are not limited to:

- Informing the EDO and the Commission if Congress, law enforcement, OGC and/or OIG are notified due to the nature of an incident.
- Informing the OPA if notification to the public is required for an incident.

6.6 NRC Users

Users should refer to the NRC Rules of Behavior for their IR responsibilities.

6.7 Office of Administration

ADM provides the policy for disciplinary action for violations of IT security policies and procedures.

6.8 Office of Public Affairs

OPA provides adequate notification to the general public when compliance with reporting requirements is necessary.

6.9 Office of General Counsel

OGC provides legal counsel, where appropriate, for incidents that require legal consultation or action.

6.10 Office of Congressional Affairs

OCA facilitates communication between NRC and Congress when a “major incident” is reported to Congress.

6.11 Office of Inspector General

OIG notifies law enforcement (e.g., FBI) if necessary for an incident.

7.0 FREQUENCY OF REVIEW

The SOB Chief is responsible for reviewing this policy at least bi-annually or upon major change(s) to the NRC infrastructure.

8.0 COGNIZANT AUTHORITY

The SOB Chief is responsible for maintaining this policy.